

**Case No. 24-6136**

---

IN THE  
**United States Court of Appeals for the Ninth Circuit**

---

J. DOE 1, et al.,  
Individually and on behalf of all others similarly situated,

*Plaintiffs and Petitioners*

v.

GITHUB, INC., et al.,

*Defendants and Respondents*

---

Petition for Permission to Appeal a Certified Order from  
the United States District Court for the Northern District of California,  
No. 4:22-cv-06823-JST, Hon. Jon S. Tigar

---

**REPLY TO GITHUB AND MICROSOFT'S OPPOSITION TO  
PETITIONERS' MOTION TO SEAL**

---

JOSEPH R. SAVERI  
**JOSEPH SAVERI LAW  
FIRM, LLP**  
601 California St., 1505  
San Francisco, CA 94108  
Telephone: (415) 500-6800  
Email:  
jsaveri@saverilawfirm.com

MATTHEW BUTTERICK  
1920 Hillhurst Avenue,  
#406  
Los Angeles, CA 90027  
Telephone: (323) 968-2632  
Email:  
mb@buttericklaw.com

MAXWELL V. PRITT  
JESSE PANUCCIO  
**BOIES SCHILLER  
FLEXNER LLP**  
44 Montgomery St., 41st FL  
San Francisco, CA 94104  
Telephone: (415) 293-6800  
Email: mpritt@bsflp.com  
jpanuccio@bsflp.com

*Attorneys for Plaintiff-Petitioners and the Proposed Class*

## TABLE OF CONTENTS

I. The District Court Repeatedly Ordered and Approved Petitioners’ Computer Code to be Redacted. ....	1
II. There Are No New Reasons to Unseal Petitioners’ Code. ....	3
III. Petitioners Meet the <i>Kamehameha</i> Standard to Justify Sealing Their Code. ....	5
A. Petitioners Have Demonstrated Reasonable Fear of Harm and are Vulnerable to Retaliation.....	7
B. Neither Respondents nor the Public Will be Prejudiced by Continuing to Seal Petitioners’ Code.....	8
IV. Conclusion.....	9

Plaintiff-Petitioners J. Does 1-5 (“Petitioners”) respectfully submit this Reply to Defendant-Respondents GitHub Inc. and Microsoft Corp.’s (“Respondents”) Opposition to Petitioners’ Motion to Maintain Seal. Dkt. 23.1. (“Opp”). Respondents seek to sweep aside the district court’s factual findings that Petitioners have a reasonable fear of violence and injury, including death, if their identities are revealed. Respondents know the identities of the Petitioners, providing them a full opportunity to defend themselves in this case. The district court’s orders protect Petitioners’ identities from public disclosure in various forms, including their unique computer code which contains specific identifying information. Once again, Respondents seek to avoid the district court’s orders in the context of disputing the Court’s ordinary sealing procedures. There is no reason to upset the procedures protecting these individuals from these substantiated threats. Recycling arguments that now failed on numerous occasions, Respondents fail to demonstrate a basis for doing so.

**I. The District Court Repeatedly Ordered and Approved Petitioners’ Computer Code to be Redacted.**

Respondents’ assertion that Petitioners have “expanded the scope of material they seek to maintain under seal beyond their names” is incorrect. Opp. at 10. Respondents ignore that the district court *repeatedly* allowed Petitioners’ computer code at issue, which contains identifying information, to be sealed in the following filings:

DOCUMENTS	
Document	Cite
First Amended Complaint	D. Ct. Dkt. 133, filed July 21, 2023
Respondents' Motion to Dismiss Petitioners' First Amended Complaint	D. Ct. Dkt. 193, filed January 16, 2024
Petitioners' Second Amended Complaint	D. Ct. Dkt. 204, filed January 30, 2024
Respondents' Motion to Dismiss Portions of the Second Amended Complaint	D. Ct. Dkt. 225, filed March 3, 2024
Respondents' Reply in Support of Their Motion to Dismiss Portions of the Second Amended Complaint	D. Ct. Dkt. 245, filed April 15, 2024

If this information were revealed, the protections afforded to Petitioners' identities would be abrogated.

As the record shows, the district court first allowed Petitioners to proceed pseudonymously based on their reasonable, demonstrable fears of actual and serious threats of violence and death directed at them and their counsel. *Doe I v. GitHub, Inc.*, 672 F. Supp. 3d 837, 854 (N.D. Cal., May 11, 2023). Then, consistent with that order, and upon a showing by Plaintiffs, the district court found good cause to allow Petitioners' computer code to be redacted and sealed in their First Amended Complaint, along with their names, because the code is unique, published in Petitioners' public GitHub repositories, and can be used to personally identify Petitioners. D. Ct. Dkt. 97, 133. The district court thereafter allowed redaction of both Petitioners' code and names in the Second Amended

Complaint and in subsequent motion to dismiss briefing D. Ct. Dkt. 193, 204, 225, 245.

Here, Petitioners move the Court to maintain the seal on Doe 1's and Doe 2's computer code that Respondents provisionally filed under sealed in their Response to Petitioners' Petition for Permission to Appeal (Dkt. 14.2, pgs.13, 24). Petitioners are moving for relief of the sort repeatedly granted by the district court.

## **II. There Are No New Reasons to Unseal Petitioners' Code.**

The petition for interlocutory appeal involves a purely legal question of whether liability under sections 1202(b)(1) and (b)(3) of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. §§ 1202(b)(1) and (b)(3), require "identity," and if so, what that means in the context of each section. Dkt. 1. But Respondents suggest that the public now needs to see Petitioners' actual code in this appeal because "no decision can provide guidance to courts and litigants if they cannot see the material allegations upon which it is based." Opp. at 2. Respondents advance this claim without any factual or logical support. The district court has also already held otherwise, finding that "[w]ithholding the true identities of the individual software developers who bring this case will not obstruct public scrutiny of the issues raised." *Doe I v. GitHub, Inc.*, 672 F. Supp. 3d at 854. This reasoning applies in equal force here. In fact, the contents of Petitioners' code is not relevant to the purely legal issue of the interpretation of the DMCA, which is

the issue certified for interlocutory review under 28 U.S.C. § 1292(b). And if it were, the identifying information present in the code can be sealed without limiting appellate review.

Beyond the important DMCA issue certified for review, Respondents now suggest that the content of Petitioners' code is somehow newly relevant and argue incoherently that the district court previously missed balancing factors in sealing that code, that now require "rebalancing." Opp. at 6. This is incorrect. After considering Petitioners' argument for sealing their code along with their names in the First Amended Complaint, D. Ct. Dkt. 97, the district court granted Petitioners' motions to seal their code, D. Ct. Dkt. 133, and then again in four subsequent orders. D. Ct. Dkt. 193, 204, 225, 245. Once again, the district court carefully considered the standing issues and found that Petitioners possessed the requisite standing under Article III. *See Doe 1 v. GitHub, Inc.*, 672 F. Supp. 3d at 849-852 (finding Petitioners have standing to pursue injunctive relief based on likely harm to intellectual property). The content of Petitioners' code is not necessary to this determination. Even if it were, these issues could be addressed by maintaining the records under seal.

Respondents identify media coverage surrounding this litigation and conclude that Petitioners' counsel "has continued to publicize the case and his involvement in it, seemingly perceiving no danger to doing so." Opp. at 8. This is

off base. This and other AI cases have garnered public attention because of the importance of the issues at stake, which is one of the reasons strongly suggesting the need for interlocutory review. In responding to such attention, Respondents and their counsel have assiduously protected the identity of their clients, consistent with the district court's order. Moreover, because Petitioners' counsel have done so, they, rather than Petitioners, have been the direct recipients of the threats brought to the district court's attention. As the district court found, "[w]hile the threatening emails were not sent to Plaintiffs directly, the emails wish death upon Plaintiffs' counsel on the basis of their involvement in this lawsuit. It is reasonable for Plaintiffs to fear that such threats might be carried out against them if their identities were to become public." *Doe 1 v. GitHub, Inc.*, 672 F. Supp. 3d at 853. There is no principled reason to disturb the district court's finding that Petitioners' fear of retaliation and violence is reasonable here.

### **III. Petitioners Meet the *Kamehameha* Standard to Justify Sealing Their Code.**

Respondents continue to assert that the Petitioners do not meet the standard for sealing and redacting under *Doe v. Kamehameha Sch./Bernice Pauahi Bishop Est.*, 596 F.3d 1036, 1042 (9th Cir. 2010). Opp. at 11. Respondents claim, "the sole basis Plaintiffs provide for sealing both their names and material allegations in the Second Amended Complaint is the desire to remain anonymous." Opp. at 8. This is at odds with the record. The district court specifically applied the *Kamehameha*

standard, indeed finding the threats of physical harm here “present the paradigmatic case for allowing anonymity.” *Doe 1 v. GitHub, Inc.*, 672 F. Supp. 3d at 852 (cleaned up, *quoting Kamehameha*, 596 F.3d at 1043). The basis, as the district court acknowledged, is Petitioners’ reasonable fear of harm based on threats of violence: “Where many individuals take the time to send private, threatening emails, it is reasonable to fear that some of those individuals might carry out their threats.” *Doe 1 v. GitHub, Inc.*, 672 F. Supp. 3d at 853.

Given the direct threats upon Petitioners’ counsel, the district court found it “reasonable for Plaintiffs to fear that such threats might be carried out against them if their identities were to become public.” *Id.* Indeed, as shown by the threats themselves, those wishing harm upon Petitioners have done so using their own contact information and without hiding their own identities, indicating a heightened threat.<sup>1</sup>

---

<sup>1</sup> Respondents’ argument that the passage of time overrides Petitioners’ reasonable fear of harm is unpersuasive. The district court found as little as seven months ago that Petitioners could continue to proceed anonymously. D. Ct. Dkt. 245, filed April 15, 2024. And indeed, the passage of time without continued threats evidences the soundness of the district court’s judgment in protecting Petitioners’ identities. Given the continued public attention of this case, there is no reason to undo these protections now.



**A. Petitioners Have Demonstrated Reasonable Fear of Harm and are Vulnerable to Retaliation.**

The Court should reject Respondents’ cavalier dismissal of death threats against Petitioners as mere “trolling.” Opp. at 11 (“These emails are the sort of odious trolling that is an unfortunate reality of the modern internet and that cannot justify proceeding in secret.”). Respondents have made this irresponsible argument before—the district court already considered and soundly rejected these arguments. *Doe 1 v. GitHub, Inc.*, 672 F. Supp. 3d at 853 (holding that “direct messages containing veiled death threats would seem to constitute behavior beyond trolling,” while noting nonetheless that “GitHub and Microsoft do not explain why the rise of internet trolls renders Plaintiffs’ fears of harm unreasonable.”). The district court held that “[t]hese were not public posts mocking or antagonizing Plaintiffs’ counsel, but rather private emails, sent directly to Plaintiffs’ counsel, wishing him and his family violent death, while using inflammatory and incendiary language.” *Id.* The court concluded, “Where many individuals take the time to send private, threatening emails, it is reasonable to fear that some of those individuals might carry out their threats.” *Id.* Other than pointing to the passage of time, which demonstrates the *success* of the steps taken, including the sealing of Petitioners’ names and code, to mitigate the receipt of violent, threatening emails, Respondents

offer no principled reason to disturb the district court's conclusions and the status quo keeping Petitioners' code sealed.

**B. Neither Respondents nor the Public Will be Prejudiced by Continuing to Seal Petitioners' Code.**

Respondents claim they will “be prejudiced by the inability to vindicate their products in view of the public,” *citing Kamehameha*, 596 F.3d at 1045 n.7. Opp. at 14. The Court should come to the same conclusion as it did in *Kamehameha*: “We doubt that anonymity would hinder the defendants’ standing defense.”

*Kamehameha*, 596 F.3d at 1045 n.7. In *Kamehameha*, the identities of the Does there were known to the Defendants. *Id.* The same is true here. As the district court held, Respondents know who the Petitioners are, and their discovery is not hindered by anonymity. *Doe I v. GitHub, Inc.*, 672 F. Supp. 3d at 853-854. Where the defendants know the plaintiffs’ names, “anonymity need not, and should not, impede either party's ability to develop its case[.]” *Id.* at 853 (internal citations and punctuation omitted). Respondents had the information necessary to assert a lack of standing, which they attempted to do, and lost. Respondents have the information necessary for this appeal.

The district court also considered and rejected Respondents’ arguments regarding prejudice to the public. Opp. at 16. The district court held that “the public interest factor does not weigh against permitting Plaintiffs to proceed pseudonymously.” *Doe I v. GitHub, Inc.*, 672 F. Supp. 3d at 854. The district court

held that “[w]ithholding the true identities of the individual software developers who bring this case will not obstruct public scrutiny of the issues raised. Plaintiffs’ names and identities have no bearing on the central issues of this case, including whether Defendants’ AI-based coding tools illegally reproduce licensed code used as training data.” *Id.*<sup>2</sup> There is no principled reason to reject the district court’s conclusion.

#### IV. Conclusion

For the foregoing reasons, the Court should grant the Petitioners’ motion (Dkt. 21) to continue to seal their computer code that Respondents provisionally filed under sealed in their Response to Petitioners’ Petition for Permission to Appeal (Dkt. 14.2, pgs.13, 24).

Dated: November 25, 2024

*s/ Joseph R. Saveri*

Joseph R. Saveri

Joseph R. Saveri  
Christopher K. L. Young  
William W. Castillo Guardado  
**JOSEPH SAVERI LAW FIRM, LLP**  
601 California Street, Suite 1505  
San Francisco, California 94108  
Telephone: (415) 500-6800  
Facsimile: (415) 395-9940  
Email: jsaveri@saverilawfirm.com

---

<sup>2</sup> Respondents’ claim that the “public would remain in the dark as to who is challenging the technology, and their basis for doing so” is incorrect. Opp. at 16. The operative complaints make it clear the Petitioners are members of the open-source code community who post their code on GitHub.

Email: cyoung@saverilawfirm.com  
Email: wcastillo@saverilawfirm.com

Matthew Butterick (State Bar No. 250953)  
1920 Hillhurst Avenue, #406  
Los Angeles, CA 90027  
Telephone: (323) 968-2632  
Facsimile: (415) 395-9940  
Email: mb@buttericklaw.com

Maxwell V. Pritt  
Joshua M. Stein  
**BOIES SCHILLER FLEXNER LLP**  
44 Montgomery Street, 41st Floor  
San Francisco, CA 94104  
Telephone: (415) 293-6800  
Email: mpritt@bsfllp.com  
Email: jstein@bsfllp.com

Jesse Panuccio  
**BOIES SCHILLER FLEXNER LLP**  
1401 New York Avenue, NW  
Washington, DC 20005  
Telephone: (202) 237-2727  
Email: jpanuccio@bsfllp.com

*Attorneys for Plaintiff-Petitioners  
and the Proposed Class*

### **CERTIFICATE OF COMPLIANCE**

This brief complies with the length limits permitted by Federal Rules of Appellate Procedure 27(d). This reply brief is 2018 words. The type size and typeface comply with Rule 32(a)(5). I further certify that this brief complies with the typeface and type-style requirements of Rule 32(a)(5)-(6) because it is printed in a proportionally spaced 14-point font, Times New Roman.

Dated: November 25, 2024

/s/ *Joseph R. Saveri*

Joseph R. Saveri